Discrete Mathematics 115 (1993) 295–298
North-Holland

Research problems

The purpose of the research problems section is the presentation of unsolved problems in discrete mathematics. Older problems are acceptable if they are not as widely known as they deserve. Problems should be submitted using the format as they appear in the journal and sent to

Professor Brian Alspach
Department of Mathematics and Statistics
Simon Fraser University
Burnaby, B.C.
Canada V5A 1S6.

Readers wishing to make comments dealing with technical matters about a problem that has appeared should write to the correspondent for that particular problem. Comments of a general nature about previous problems should be sent to Professor Alspach.

Problems 169–171.

Correspondent: Dušan B. Jevtić
Department of Mathematical Sciences
University of Alaska Fairbanks
Fairbanks, AK 99775-1110
USA.

Shannon wrote [1, p. 641], "In another paper we will discuss the case of a channel with two or more terminals having inputs only and one terminal with an output only, a case for which a complete and simple solution of a capacity region has been found." This channel has later been called the multiple-access channel (MAC). Below we present a code-design problem for a noiseless OR MAC.

Let $\mathscr{X}_n^{(k)}$ denote the set of all k-element subsets of $\mathscr{X}_n \triangleq \{1,2,3,\ldots,n\}$. Further, let $2^{\mathscr{X}_n}$ denote the power set of $\mathscr{X}_n$ and let $|\mathscr{X}|$ stand for the number of elements in $\mathscr{X} \subseteq \mathscr{X}_n$.

A *codebook of order* T is a collection $\{\mathscr{P}_1, \mathscr{P}_2, \ldots, \mathscr{P}_T\}$ such that $\mathscr{P}_i = \{\emptyset\} \cup \mathscr{E}_i$ where $\mathscr{E}_i \subset \mathscr{X}_n^{(k)}$ and $\mathscr{E}_i \cap \mathscr{E}_j = \emptyset$ for $i \neq j$. A set $B \in \mathscr{P}_i$ is called a *codeword*. Thus a codeword is either $\emptyset$ or a hyperedge from a k-graph $(\mathscr{X}_n, \mathscr{E}_i)$.

Let $\mathscr{P} = \mathscr{P}_1 \times \mathscr{P}_2 \times \cdots \times \mathscr{P}_T$ and let $F: \mathscr{P} \to 2^{\mathscr{X}_n}$ be defined as

$$F(A_1, A_2, \ldots, A_T) \triangleq A_1 \cup A_2 \cup \cdots \cup A_T, \quad A_i \in \mathscr{P}_i.$$

A codebook $\{\mathscr{P}_1, \mathscr{P}_2, \ldots, \mathscr{P}_T\}$ is said to be *uniquely decodable* if for any T-tuple $(A_1, A_2, \ldots, A_T)$ from $\mathscr{P}$ and any codeword $B \neq \emptyset, B \subseteq F(A_1, A_2, \ldots, A_T)$ implies $B = A_i$ for some $i \in \{1, 2, \ldots, T\}$. Put another way, a codebook $\{\mathscr{P}_1, \mathscr{P}_2, \ldots, \mathscr{P}_T\}$ is uniquely decodable if any set $F(A_1, A_2, \ldots, A_T)$ has a unique inverse with respect to each $\mathscr{P}_i$.

If $\{\mathscr{P}_1, \mathscr{P}_2, \ldots, \mathscr{P}_T\}$ is uniquely decodable, then F is an injection. The converse is not true. For example, if $\mathscr{P}_1 = \{\emptyset, \{3,4\}, \{2,5\}\}$ and $\mathscr{P}_2 = \{\emptyset, \{1,3\}, \{3,5\}\}$, then $\{\mathscr{P}_1, \mathscr{P}_2\}$ is not uniquely decodable. (Take $A_1 = \{2,5\}$ and $A_2 = \{1,3\}$. Then, $A_1 \cup A_2 = \{1,2,3,5\}$ and $B = \{3,5\}$ satisfies $B \subset A_1 \cup A_2$ and $B \neq A_i, i = 1, 2$. However, the nine sets $A_i \cup A_j$, where $A_i \in \mathscr{P}_1$ and $A_j \in \mathscr{P}_2$, are different elements of $2^{\mathscr{X}_5}$.)

The *rate* R_i of a *component* $\mathscr{P}_i$ is defined by $|\mathscr{P}_i| = 2^{nR_i}$. The *rate sum* of a T-component codebook on $\mathscr{X}_n^{(k)}$, denoted by $R_T(k,n)$, is the sum of its component rates, i.e., $R_T(k,n) \triangleq R_1 + R_2 + \cdots + R_T$. Rate sum is an information-theoretic measure of the relative size of $|\mathscr{P}|$. A uniquely decodable codebook of order T on $\mathscr{X}_n^{(k)}$ is *optimum* if its rate sum is maximum for given n, k, and T.

Let $\{\mathscr{P}_1, \mathscr{P}_2, \ldots, \mathscr{P}_T\}$ be a uniquely decodable codebook on $\mathscr{X}_n^{(k)}$ such that $|\mathscr{P}_i| > 1$ for all i and let

$$\beta_T(k,n) \triangleq 1 + \binom{n}{k} + \binom{n}{k+1} + \cdots + \binom{n}{kT}.$$

Then,

(a) The 2^T sets $\bigcup_{i=1}^T (E_i \cap A_i)$, where $E_i \in \{\emptyset, \mathscr{X}_n\}$ and $A_i \in \mathscr{P}_i$, are all distinct. Hence, by pigeonhole principle, $2^T \leqslant |F(\mathscr{P})|$ and since $|\mathscr{P}| = |F(\mathscr{P})|$ we have $R_T(k,n) \geqslant n^{-1} T$.

(b) The possible distinct images of $\mathscr{P}$ under F are $\emptyset$ and all subsets of $\mathscr{X}_n$ with no less than k elements and no more than $\min\{kT, n\}$ elements. Hence, $|F(\mathscr{P})| \leqslant \beta_T(k,n)$ and, due to $|\mathscr{P}| = |F(\mathscr{P})|$, we have $R_T(k,n) \leqslant n^{-1} \log_2 \beta_T(k,n)$. Furthermore, $2^T \leqslant |F(\mathscr{P})|$ implies $T \leqslant \log_2 \beta_T(k,n)$.

Let $T = n$ and $k = 1$. Then, by (a) and (b) above, $R_n(1,n) = 1$. Thus, $\mathscr{P}_i = \{\emptyset, \{i\}\}$, $i = 1, \ldots, n$, is an optimum codebook. By (b) above, this is the only codebook on $\mathscr{X}_n^{(k)}$ with rate sum equal to one.

Problem 169. (Posed by Claude Shannon.) Find an optimum uniquely decodable codebook of order T on $\mathscr{X}_n^{(k)}$ for given $n > 4$, $k > 1$, and $T > 1$.

Spread-spectrum codebooks

A codebook $\{\mathscr{P}_1, \mathscr{P}_2, \ldots, \mathscr{P}_T\}$ on $\mathscr{X}_n^{(k)}$ is said to have a *spread-spectrum property* (SSP) if for any vertex $j \in \mathscr{X}_n$ there is, in each k-graph $\mathscr{P}_i - \{\emptyset\}$, at least one hyperedge incident with j.

Clearly SSP implies that $\bigcup_{j=1}^{r} E_{i_j} = \mathscr{X}_n$, where $E_{i_1}, E_{i_2}, \ldots, E_{i_{r_j}}, r_j = |\mathscr{P}_j|$, are codewords from $\mathscr{P}_j$, $j = 1, 2, \ldots, T$.

Example 1. If $\mathscr{P}_1^* = \{\emptyset, \{1,2\}, \{3,4\}\}$ and $\mathscr{P}_2^* = \{\emptyset, \{1,3\}, \{2,4\}\}$, then $\{\mathscr{P}_1^*, \mathscr{P}_2^*\}$ is an optimum uniquely decodable SSP codebook on $\mathscr{X}_4^{(2)}$. Sets $\emptyset, \{1,2\}$ and $\{3,4\}$ are codewords from $\mathscr{P}_1^*$. Further, $R_i = 4^{-1}\log_2 3, i=1,2$, and $R_1+R_2 \approx 0.792$. (By (a) and (b) above, $0.5 \leqslant R_2(2,4) \leqslant 0.896$ for any uniquely decodable codebook on $\mathscr{X}_4^{(2)}$.)

SSP implies that $\{\mathscr{E}_1, \mathscr{E}_2, \ldots, \mathscr{E}_T\}, \mathscr{E}_i = \mathscr{P}_i - \{\emptyset\}$, is at least 1-mutually-intersecting-family of T k-graphs. Hence, if $\{\mathscr{P}_1, \mathscr{P}_2, \ldots, \mathscr{P}_T\}$ is a uniquely decodable codebook, then $T \leqslant k$ follows at once. Below we prove a bit stronger assertion.

Lemma 1. *Let $\{\mathscr{P}_1, \mathscr{P}_2, \ldots, \mathscr{P}_T\}$ be a uniquely decodable SSP codebook on $\mathscr{X}_n^{(k)}$. Further, let $\mu_i = \max\{|E_{i_l} \cap E_{i_m}| : E_{i_l}, E_{i_m} \in \mathscr{P}_i\}$ and let μ be the largest such μ_i for $i=1,\ldots,T$. Then, $T \leqslant k-\mu$.*

Proof. Without loss of generality we may assume $\mu=\mu_1$. Let $\mathscr{E}_i = \mathscr{P}_i - \{\emptyset\}$. If E_{1_y} and E_{1_z} are two different edges from $\mathscr{E}_1$ incident with μ vertices $j_1, j_2, \ldots, j_\mu$ from $\mathscr{X}_n$, then we can write $E_{1_y} = \{j_1, j_2, \ldots, j_\mu, y_{\mu+1}, \ldots, y_k\}$ and $E_{1_z} = \{j_1, j_2, \ldots, j_\mu, z_{\mu+1}, \ldots, z_k\}$. If $T=k-\mu+1$, then, due to SSP, we can choose an edge E_i incident with $y_{\mu+i-1}$ from each $\mathscr{E}_i$ for $i=2,3,\ldots,k-\mu+1$. Let $\bar{E} = (E_{1_z}, E_2, \ldots, E_{k-\mu+1})$. Then, $E_{1_y} \subset F(\bar{E})$ and so constructed codebook $\{\mathscr{P}_1, \ldots, \mathscr{P}_{k-\mu+1}\}$ is not uniquely decodable. Thus $T < k-\mu+1$. $\square$

According to Lemma 1, $T=k$ only if the edges of each k-graph $\mathscr{E}_i$ are vertex disjoint. This implies at most $(1+\lfloor n/k \rfloor)$ codewords in each $\mathscr{P}_i$ (1 is for $\emptyset$). Furthermore, if $T=k$, then there is in each $\mathscr{E}_i$ exactly one edge incident with a given vertex from $\mathscr{X}_n$.

Corollary 1. *The maximum order of a uniquely decodable SSP codebook on $\mathscr{X}_n^{(k)}$ is k. The corresponding rate sum cannot exceed $\lambda\log_2(1+\lambda^{-1})$, where $\lambda n = k = T$.*

An example of a codebook which meets the upper bound on the rate sum in the above corollary is a collection of k parallel pencils of an affine plane π_k of order k. (There are $\binom{k+1}{k}$ such codebooks.) Then, $T=k$ and $n=k^2$ and the rate sum is $R_{\pi_k} \triangleq k^{-1}\log_2(1+k)$.

If k^2+k lines of π_k are partitioned into T components of a $\{\mathscr{P}_1, \mathscr{P}_2, \ldots, \mathscr{P}_T\}$, the maximum resulting rate sum is

$$R_T(k,k^2) = \frac{T}{k^2}\log_2\left(1+\frac{k^2+k}{T}\right).$$

By using the notion of a distinguishable point, it was shown in [2] that this codebook is uniquely decodable if and only if $T \leqslant k-1$.

Problem 170. (Posed by Hasan K. Alkhatib and Dušan B. Jevtić.) One can show that $R_T(k,k^2) < R_{\pi_k}$ for $T<k$. Is it true that the rate sum of a uniquely decodable SSP codebook on $\mathscr{X}_n^{(k)}$ cannot exceed $\lambda\log_2(1+\lambda^{-1})$, $\lambda n = k$, for any $T<k$?

Problem 171. (Posed by Dušan B. Jevtić.) $\mathscr{A} \subset 2^{\mathscr{X}_n}$ and $\mathscr{B} \subset 2^{\mathscr{X}_n}$ are two r-mutually-intersecting families on $\mathscr{X}_n$ if $A \in \mathscr{A}$ and $B \in \mathscr{B}$ imply $|A \cap B| = r$. Given r, $1 < r < k$, find the maximum rate sum of a uniquely decodable codebook $\{\mathscr{P}_1, \mathscr{P}_2, \ldots, \mathscr{P}_T\}$ on $\mathscr{X}_n^{(k)}$ where $\{\mathscr{P}_i - \{\emptyset\}: i = 1, \ldots, T\}$ is an r-mutually-intersecting family.

Design of r-mutually-intersecting SSP codebooks was discussed in [3]. An optimum codebook has not been found.

The description of a coding problem via k-graphs and the definition of a spread-spectrum codebook, as well as the simple facts stated above are new. They are, however, application driven. By identifying: (1) a subset A of $\mathscr{X}_n$ with the characteristic function $\mathscr{X}_A$ of A on $\mathscr{X}_n$, and (2) $\cup$ with the bitwise logical OR of elements from $\{0,1\}^n$, we have described a problem relating to the binary OR MAC with non-cooperative users.

References

[1] C.E. Shannon, Two-way communication channels, in: Proc. 4th Berkeley Symp. Math. Statist. and Prob., Vol. 1 (1961) 611–644; reprinted in: D. Slepian, ed., Key Papers in the Development of Information Theory (IEEE Press, New York, 1974) 339–372.

[2] D.B. Jevtić and H.S. Alkhatib, Frequency hopping codes for multiple-access channels: a geometric approach, IEEE Trans. Info. Theory 35 (1989) 477–481.

[3] D.B. Jevtić, Well structured FHMA codebooks: a geometric approach, IEEE Trans. Comm., to appear.